<table>
<thead>
<tr>
<th>Title</th>
<th>On a distribution property of the residual order of $a$ (mod $p$) (III) (Diophantine Problems and Analytic Number Theory)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Murata, Leo; Chinen, Koji</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2003), 1319: 139-147</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2003-05</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/43059">http://hdl.handle.net/2433/43059</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

京都大学学術情報リポジトリ
On a distribution property of the residual order of \( a(\text{mod } p) \), III

Leo Murata* and Koji Chinen†

1 Introduction

Let \( N \) be the set of all natural numbers, \( P \) the set of all prime numbers. And \( p \) always denotes a prime number, \( \pi(x) \) the number of primes not exceeding \( x \).

For a fixed natural number \( a \geq 2 \), we can define two functions, \( I_a \) and \( D_a \), from \( P \) to \( N \):

\[
I_a : p \mapsto I_a(p) = |(\mathbb{Z}/p\mathbb{Z})^\times : \langle a \pmod{p} \rangle| \\
\text{(the residual index of } a \pmod{p}),
\]

\[
D_a : p \mapsto D_a(p) = \#(a \pmod{p}) \\
\text{(the residual order of } a \pmod{p} \text{ in } (\mathbb{Z}/p\mathbb{Z})^\times),
\]

where \( (\mathbb{Z}/p\mathbb{Z})^\times \) denotes the set of all invertible residue classes modulo \( p \), and \( | : | \) the index of the subset.

We have a simple relation

\[
I_a(p) \ D_a(p) = p - 1,
\]

but both of these functions fluctuate quite irregularly. More than 200 years ago, C. F. Gauss calculated these numbers and he already noticed that

(a) The movement of \( I_{10} \) is much more modest than \( D_{10} \),
(b) \( I_{10}(p) = 1 \) happens rather frequently.

*Department of Mathematics, Faculty of Economics, Meiji Gakuin University, 1-2-37 Shirokanedai, Minato-ku, Tokyo 108-8636, Japan. E-mail: leo@eco.meijigakuin.ac.jp
†Department of Mathematics, Faculty of Engineering, Osaka Institute of Technology. Omiya, Asahi-ku, Osaka 535-8585, Japan. E-mail: YHK03302@nifty.ne.jp
So he studied only about the distribution property of $I_a(p)$ and conjectured that

$$\#\{p \in \mathbb{P} : I_{10}(p) = 1\} = \infty,$$

which is now a part of so-called Artin's conjecture for primitive root.

Let us define the set, for a natural number $n$,

$$N_a(x; n) = \{p \leq x ; I_a(p) = n\},$$

then we already knows that

**Theorem A** ([5],[6]) *We assume the Generalized Riemann Hypothesis (GRH). Then*

$$\#N_a(x; n) = C_a^n \pi(x) + O\left(\frac{x \log \log x}{\log^2 x}\right),$$

*where $C_a^n$ is a computable constant depends only on $a$ and $n$. and

**Corollary 1** *We assume GRH. When $a$ is square-free and $a \not\equiv 1 \pmod{4}$, the map $I_a$ is surjective from $\mathbb{P}$ to $\mathbb{N}$. And on the map $D_a$, we have

**Theorem B** The map $D_a$ is almost surjective from $\mathbb{P}$ to $\mathbb{N}$. Where "almost surjective" means "except for only finite members of $n$'s". But we notice a big difference between these two surjectivities. For any $n \in \mathbb{N}$, the set

$$D_a^{-1}\{n\} = \{p \in \mathbb{P} ; D_a(p) = n\}$$

contains only a finite number of elements. In fact, if $D_a(p) = n$, then

$$n + 1 \leq p \leq a^n.$$ 

On the contrary, Theorem A shows that (under GRH),

$$I_a^{-1}\{n\} = \{p \in \mathbb{P} ; I_a(p) = n\} \sim C_a^{(n)} \text{ times of } \mathbb{P}.$$ 

So, the map $I_a(p)$ covers $\mathbb{N}$ very *thickly*, while the map $D_a(p)$ covers $\mathbb{N}$ very *thinly*. Here we want to study distribution properties of $D_a(p)$. Then taking into account of the above facts, we think we should take a subset $S$ of $\mathbb{N}$ which contains *infinitely* many elements, and consider the inverse image

$$D_a^{-1}(S) = \{p \leq x ; D_a(p) \in S\}.$$

In this note, in Section 2 we take $S = \{a \text{ residue class in } \mathbb{N}\}$ (joint work of K. Chinen and L. Murata), and in Section 3 we take $S = \mathbb{P}$ (joint work of C. Pomerance and L. Murata).
2 The case $S = a$ residue class in $\mathbb{N}$

This part is a sequel of our previous works [1], [2]. See also [3], [7].

2.1 A residue class mod 4

Let us take $S$ as a residue class mod 4. Namely we define, for $l = 0, 1, 2, 3$,

$$Q_a(x; 4, l) = \{ p \leq x ; D_a(p) \equiv l \pmod{4} \}.$$ 

Then, in our previous paper, we proved

**Theorem 1** ([7]) We assume $a \in \mathbb{N}$ is not a perfect $h$-th power with $h \geq 2$, and put

$$a = a_1 a_2^2, \quad a_1 : \text{square free}.$$ 

When $a_1 \equiv 2 \pmod{4}$, we define $a'_1$ by

$$a_1 = 2a'_1.$$ 

We assume GRH. And we define an absolute constant $C$ by

$$C = \prod_{p \equiv 3 \pmod{4}} \left(1 - \frac{2p}{(p^2 + 1)(p - 1)}\right).$$

Then, for $l = 1, 3$, we have an asymptotic formula

$$\# Q_a(x; 4, l) = \delta_l \pi(x) + O\left(\frac{x}{\log x \log \log x}\right),$$

and the leading coefficients (=the natural density) $\delta_l$ ($l = 1, 3$) are given by the following way:

(I) If $a_1 \equiv 1, 3 \pmod{4}$, then $\delta_1 = \delta_3 = \frac{1}{6}$.

(II) When $a_1 \equiv 2 \pmod{4}$,

(i) If $a'_1 = 1$, i.e. $a = 2 \cdot (a \text{ square number})$, then

$$\delta_1 = \frac{7}{48} - \frac{C}{8}, \quad \delta_3 = \frac{7}{48} + \frac{C}{8}.$$ 

(ii) If $a'_1 \equiv 1 \pmod{4}$ with $a'_1 > 1$, then

(ii-1) if $a'_1$ has a prime divisor $q$ with $q \equiv 1 \pmod{4}$, then $\delta_1 = \delta_3 = \frac{1}{6}$.
(ii-2) if all prime divisors $q$ of $a_1'$ satisfy $q \equiv 3 \pmod{4}$, then

$$
\begin{align*}
\delta_1 &= \frac{1}{6} - \frac{C}{8} \prod_{p|a_1'} \left( \frac{-2p}{p^3 - p^2 - p - 1} \right), \\
\delta_3 &= \frac{1}{6} + \frac{C}{8} \prod_{p|a_1'} \left( \frac{-2p}{p^3 - p^2 - p - 1} \right).
\end{align*}
$$

(iii) If $a_1' \equiv 3 \pmod{4}$, then

(iii-1) if $a_1'$ has a prime divisor $q$ with $q \equiv 1 \pmod{4}$, then $\delta_1 = \delta_3 = \frac{1}{6}$,

(iii-2) if all prime divisors $q$ of $a_1'$ satisfy $q \equiv 3 \pmod{4}$, then

$$
\begin{align*}
\delta_1 &= \frac{1}{6} + \frac{C}{8} \prod_{p|a_1'} \left( \frac{-2p}{p^3 - p^2 - p - 1} \right), \\
\delta_3 &= \frac{1}{6} - \frac{C}{8} \prod_{p|a_1'} \left( \frac{-2p}{p^3 - p^2 - p - 1} \right).
\end{align*}
$$

This theorem shows that, roughly speaking, usually we have rather beautiful distribution

$$
\begin{align*}
\#Q_a(x; 4, 0) &\sim \frac{1}{3} \pi(x) \quad \text{unconditional} \\
\#Q_a(x; 4, 1) &\sim \frac{1}{6} \pi(x) \\
\#Q_a(x; 4, 2) &\sim \frac{1}{3} \pi(x) \\
\#Q_a(x; 4, 3) &\sim \frac{1}{6} \pi(x) \quad \text{we need GRH}
\end{align*}
$$

And we notice that when $(a_1, 4) > 1$ the distribution turns into a little irregular one. Anyway it seems an interesting phenomenon, in II-(ii) and II-(iii), the densities $\delta_1$ and $\delta_3$ are controled by whether $a_1'$ has a prime factor $q$ with $q \equiv 1 \pmod{4}$ or not.

For numerical examples, see Section 4, Table 4.1 - Table 4.3.

Then, what happens for another modulus?

### 2.2 A residue class mod 5

We can not find a good probabilistic model for this problem so far, i.e. we do not know why the natural density of $Q_a(x; 4, 1)$ should be equal to $\frac{1}{6}$?

But here we remark that this problem has a relation to the structure of the additive group $\mathbb{Z}/4\mathbb{Z}$. 
$Z/4\mathbb{Z} = \{0, 1, 2, 3\} \sim \#Q_a(x; 4, Z/4\mathbb{Z}) \sim \pi(x)$

\[ \cup \{0, 2\} \sim \#Q_a(x; 4, 0 \cup 2) \sim \frac{2}{3}\pi(x) \]

\[ \cup \{0\} \sim \#Q_a(x; 4, 0) \sim \frac{1}{3}\pi(x) \]

And in order to separate $\bar{1}$ and $\bar{3}$, we need GRH.

Then, since $Z/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ has only one additive subgroup $\{0\}$, we can expect that we can get an asymptotic formula for $\#Q_a(x; 5, 0)$ and we need GRH to get an asymptotic formula for $\#Q_a(x; 4, j)$ for $j = 1, 2, 3, 4$. And it is true.

Here we show our result only some simple cases. Namely we assume $a \in \mathbb{N}$ is not a perfect $h$-th power with $h \geq 2$, and put

\[ a = a_1a_2^2, \quad a_1 : \text{square free}, \]

as above, and further assume $5 \nmid a_1$ — as we remarked already, when $5 \mid a_1$, we have rather irregular densities.

**Theorem 2** Let $G$ be the multiplicative group of all characters modulo 5. We define, for $\chi \in G$, the numbers $\beta_\chi$ and $C_\chi$ by

\[ \beta_\chi = \begin{cases} 1, & \chi \in G^2, \\ -1, & \text{otherwise}, \end{cases} \]

and

\[ C_\chi = \prod_{p \neq 5} \frac{p^3 - p^2 - p + \chi(p)}{(p-1)(p^2 - \chi(p))}. \]

(1) If $j = 0$, then we have an asymptotic formula unconditionally

\[ \#Q_a(x; 5, 0) = \frac{5}{24}\pi(x) + O\left(\frac{x}{\log x \log \log x}\right). \]

(II) When $j \neq 0$, we assume GRH. Then we have

\[ \#Q_a(x; 5, j) = \delta_j \pi(x) + O\left(\frac{x}{\log x \log \log x}\right), \]

and the leading coefficient is given by

(II-1) If $a_1 \equiv 1 \pmod{4}$, then

\[ \delta_j = \frac{25}{96} - \frac{1}{16} \sum_{\chi \in G} \beta_\chi \chi(j) C_\chi \left(1 + \prod_{p|2a_1} \frac{p \chi(p) - 1}{p^3 - p^2 - p + \chi(p)}\right). \]
(II-2) If \(a_1 \equiv 2 \pmod{4}\), then
\[
\delta_j = \frac{25}{96} - \frac{1}{16} \sum_{\chi \in G} \beta_{\chi} \chi(j) C_{\chi} \left( 1 + \frac{\chi(2)^2}{16} \prod_{p|2a_1} \frac{p (\chi(p) - 1)}{p^3 - p^2 - p + \chi(p)} \right).
\]

(II-3) If \(a_1 \equiv 3 \pmod{4}\), then
\[
\delta_j = \frac{25}{96} - \frac{1}{16} \sum_{\chi \in G} \beta_{\chi} \chi(j) C_{\chi} \left( 1 + \frac{\chi(2)}{4} \prod_{p|2a_1} \frac{p (\chi(p) - 1)}{p^3 - p^2 - p + \chi(p)} \right).
\]

We can prove this theorem by the similar method which we used in \([7]\), but in order to separate four classes — 1, 2, 3, 4 — we need Dirichlet characters and very complicated calculations.

We can extend this result to much more general moduli, such as \(q^r\) with a prime \(q\) (see \([4]\)).

For \(\chi \notin G^2\), the number \(C_{\chi}\) is not a real number. The most interesting feature of this result may be the fact that a combination of these complex numbers gives the real density of \(\#Q_a(x;5,j)\).

For numerical examples, see Section 4, Table 4.4 - Table 4.6.

3 The case \(S = P\)

Here we take \(a = 2\), and consider the set
\[
M(x) = \{ p \leq x \mid I_2(p) \text{ is prime}\}.
\]

On the cardinality of this set, Pomerance \([9]\) proved

**Theorem C** We have unconditionally
\[
\#M(x) \ll \pi(x) \frac{\log \log \log x}{\log \log x},
\]

and under GRH,
\[
\#M(x) \ll \pi(x) \frac{\log \log x}{\log x}.
\]

We can improve the latter estimate as follows:

**Theorem 3** ([8]) We assume GRH. Then we have
\[
\#M(x) \ll \pi(x) \frac{1}{\log x}.
\]
Here we remark that, this estimate seems to be best possible. In fact, let us consider the set
\[ L(x) = \{ p \leq x ; \, \frac{p-1}{2} \text{ is also prime, } p \equiv 7 \pmod{8} \}. \]
Then, it is easy to see that \( L(x) \subset M(x) \), and it is (not yet proved but) conjectured that
\[ \# L(x) \sim C \pi(x) \frac{1}{\log x} \]
with a strictly positive constant \( C \), which gives a lower bound of \( \# M(x) \).
For the proof, see [8].

4 Some numerical examples

Here we show some numerical examples to compare our theoretical results with experimental results.

In the Tables 4.1 - 4.3, we compare the theoretical densities and the experimental densities \( \pi(x)^{-1} \# Q_a(x; 4, j) \) for \( x = 10^3, 10^4, 10^5, 10^6, 10^7 \).

### Table 4.1. The densities of \( Q_5(x; 4, l) \)
Theoretical densities are typical \( \left( \frac{1}{3}, \frac{1}{6}, \frac{1}{3}, \frac{1}{6} \right) \).

<table>
<thead>
<tr>
<th>( x )</th>
<th>( l = 0 )</th>
<th>( l = 1 )</th>
<th>( l = 2 )</th>
<th>( l = 3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^3 )</td>
<td>0.319277</td>
<td>0.156627</td>
<td>0.349398</td>
<td>0.174699</td>
</tr>
<tr>
<td>( 10^4 )</td>
<td>0.327628</td>
<td>0.167074</td>
<td>0.340668</td>
<td>0.164629</td>
</tr>
<tr>
<td>( 10^5 )</td>
<td>0.334619</td>
<td>0.167049</td>
<td>0.333055</td>
<td>0.165276</td>
</tr>
<tr>
<td>( 10^6 )</td>
<td>0.333227</td>
<td>0.167155</td>
<td>0.332934</td>
<td>0.166684</td>
</tr>
<tr>
<td>( 10^7 )</td>
<td>0.333320</td>
<td>0.166771</td>
<td>0.333099</td>
<td>0.166810</td>
</tr>
</tbody>
</table>

### Table 4.2. The densities of \( Q_{50}(x; 4, l) \)
Theoretical densities are \( \left( \frac{5}{12}, \frac{7}{48} - \frac{C}{8} \approx 0.06538, \frac{7}{24}, \frac{7}{48} + \frac{C}{8} \approx 0.22629 \right) \).

<table>
<thead>
<tr>
<th>( x )</th>
<th>( l = 0 )</th>
<th>( l = 1 )</th>
<th>( l = 2 )</th>
<th>( l = 3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^3 )</td>
<td>0.415663</td>
<td>0.036145</td>
<td>0.295181</td>
<td>0.253012</td>
</tr>
<tr>
<td>( 10^4 )</td>
<td>0.409943</td>
<td>0.068460</td>
<td>0.290139</td>
<td>0.231459</td>
</tr>
<tr>
<td>( 10^5 )</td>
<td>0.416684</td>
<td>0.065172</td>
<td>0.292284</td>
<td>0.225860</td>
</tr>
<tr>
<td>( 10^6 )</td>
<td>0.416569</td>
<td>0.065889</td>
<td>0.291633</td>
<td>0.225910</td>
</tr>
<tr>
<td>( 10^7 )</td>
<td>0.416719</td>
<td>0.065351</td>
<td>0.291584</td>
<td>0.226345</td>
</tr>
</tbody>
</table>
Table 4.3. The densities of $Q_6(x; 4, l)$

Theoretical densities are $\left(\frac{1}{3}, \frac{1}{6} - \frac{3C}{56} \approx 0.13219, \frac{1}{3}, \frac{1}{6} + \frac{3C}{56} \approx 0.20115\right)$.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$l = 0$</th>
<th>$l = 1$</th>
<th>$l = 2$</th>
<th>$l = 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^3$</td>
<td>0.331325</td>
<td>0.126506</td>
<td>0.325301</td>
<td>0.216867</td>
</tr>
<tr>
<td>$10^4$</td>
<td>0.334963</td>
<td>0.133659</td>
<td>0.333333</td>
<td>0.198044</td>
</tr>
<tr>
<td>$10^5$</td>
<td>0.333785</td>
<td>0.133577</td>
<td>0.332847</td>
<td>0.199791</td>
</tr>
<tr>
<td>$10^6$</td>
<td>0.333151</td>
<td>0.132249</td>
<td>0.333507</td>
<td>0.201093</td>
</tr>
<tr>
<td>$10^7$</td>
<td>0.333331</td>
<td>0.132179</td>
<td>0.333019</td>
<td>0.201471</td>
</tr>
</tbody>
</table>

Here are some examples where the modulus is 5. In the following tables, the second row shows the theoretical density.

Table 4.4. The densities of $Q_{21}(x; 5, l)$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$l = 0$</th>
<th>$l = 1$</th>
<th>$l = 2$</th>
<th>$l = 3$</th>
<th>$l = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^3$</td>
<td>0.208333</td>
<td>0.235494</td>
<td>0.176925</td>
<td>0.233715</td>
<td>0.145532</td>
</tr>
<tr>
<td>$10^4$</td>
<td>0.193939</td>
<td>0.266667</td>
<td>0.163636</td>
<td>0.260606</td>
<td>0.120482</td>
</tr>
<tr>
<td>$10^5$</td>
<td>0.209625</td>
<td>0.242251</td>
<td>0.166395</td>
<td>0.235726</td>
<td>0.145069</td>
</tr>
<tr>
<td>$10^6$</td>
<td>0.210554</td>
<td>0.242048</td>
<td>0.174054</td>
<td>0.230160</td>
<td>0.147862</td>
</tr>
<tr>
<td>$10^7$</td>
<td>0.208179</td>
<td>0.236091</td>
<td>0.176457</td>
<td>0.233251</td>
<td>0.143472</td>
</tr>
<tr>
<td>$10^8$</td>
<td>0.208218</td>
<td>0.236068</td>
<td>0.176878</td>
<td>0.233708</td>
<td>0.144110</td>
</tr>
</tbody>
</table>

Table 4.5. The densities of $Q_6(x; 5, l)$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$l = 0$</th>
<th>$l = 1$</th>
<th>$l = 2$</th>
<th>$l = 3$</th>
<th>$l = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^3$</td>
<td>0.208333</td>
<td>0.233302</td>
<td>0.179043</td>
<td>0.234686</td>
<td>0.144636</td>
</tr>
<tr>
<td>$10^4$</td>
<td>0.204819</td>
<td>0.289157</td>
<td>0.192771</td>
<td>0.198795</td>
<td>0.114458</td>
</tr>
<tr>
<td>$10^5$</td>
<td>0.215974</td>
<td>0.246944</td>
<td>0.175224</td>
<td>0.231459</td>
<td>0.130399</td>
</tr>
<tr>
<td>$10^6$</td>
<td>0.208133</td>
<td>0.231283</td>
<td>0.181335</td>
<td>0.231178</td>
<td>0.148071</td>
</tr>
<tr>
<td>$10^7$</td>
<td>0.208571</td>
<td>0.232840</td>
<td>0.179219</td>
<td>0.235362</td>
<td>0.144007</td>
</tr>
<tr>
<td>$10^8$</td>
<td>0.208645</td>
<td>0.233330</td>
<td>0.179161</td>
<td>0.234770</td>
<td>0.144093</td>
</tr>
</tbody>
</table>

Table 4.6. The densities of $Q_3(x; 5, l)$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$l = 0$</th>
<th>$l = 1$</th>
<th>$l = 2$</th>
<th>$l = 3$</th>
<th>$l = 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^3$</td>
<td>0.208333</td>
<td>0.238076</td>
<td>0.169818</td>
<td>0.235252</td>
<td>0.148521</td>
</tr>
<tr>
<td>$10^4$</td>
<td>0.210843</td>
<td>0.210843</td>
<td>0.168747</td>
<td>0.259036</td>
<td>0.132530</td>
</tr>
<tr>
<td>$10^5$</td>
<td>0.211084</td>
<td>0.238794</td>
<td>0.160554</td>
<td>0.234719</td>
<td>0.154849</td>
</tr>
<tr>
<td>$10^6$</td>
<td>0.208238</td>
<td>0.241397</td>
<td>0.164964</td>
<td>0.235036</td>
<td>0.150365</td>
</tr>
<tr>
<td>$10^7$</td>
<td>0.208125</td>
<td>0.238687</td>
<td>0.169448</td>
<td>0.234725</td>
<td>0.149014</td>
</tr>
<tr>
<td>$10^8$</td>
<td>0.208340</td>
<td>0.238100</td>
<td>0.169499</td>
<td>0.235312</td>
<td>0.148749</td>
</tr>
</tbody>
</table>
References


